19 ビジネス分野における業務要件の形式的検証技術

森岡　剛・三部良太（(株)日立製作所）

業務とシステムの整合性保証の困難さ

2010 年代に向け，ビジネス環境の変化は速度を増してゆく．複雑化する業務を短いリードタイムで実現する能力が企業の生き残りにとって重要となる．業務の要件を手戻りなく正確に情報システムによって実現するには，仕様レベルでの高い品質の保証が求められる．

業務の要件は一般に，企業活動を規制する各種の法制度や業界のルール，業務手順やシステム運用手順などに含まれている．仕様レベルでの確認が必要な業務要件の例としては，正しい処理順序や処理のタイミング，データ送受信の内容，他のリソースへのアクセス手順（認証や証跡に関する手順も含む），副作用の不在などがある．

仕様レベルでの業務とシステムの整合確認には人手による目視レビューが一般的であるが，その属人性が問題となる．個々の要件の確認が容易であっても，大規模開発における数千から数万の項目の網羅的確認や，要件変更・仕様変更の際の回帰的なレビューの実施は大きな困難が伴う．

業務要件と仕様の整合性確認を自動化する技術が望まれる．近年，数学的手法による網羅的な確認によってシステムの高品質を保証する技術である形式手法への期待が高まっているが，ビジネス分野におけるその有効な適用方法はいまだ模索中の段階にある．本稿では業務要件検証への形式手法の効果的な適用のイメージを述べる．

形式手法適用の課題

図 -1 は従来の形式手法適用イメージである．検証担当者は，業務要件とシステム仕様を踏まえ，数学的に厳密な検証用モデルを作成する．形式検証器は自動または半自動で検証処理を行い，その結果を出力する．形式検証器としては，システムの動的な振る舞いのモデルを対象とするモデル検査ツール（Spin など）や，関数言語的に記述した形式仕様を対象とする形式仕様検証ツール(B メソッドなど)など多くのツールが存在する．

従来の適用イメージの課題の第 1 は，検証用モデルが特定の形式検証器の入力形式と特定の検証目的を反映した「一品ものモデル」である点である．検証目的ごとに検証用モデルが必要であるが，その作成には高度なスキルが要求される．また，検証目的やシステム仕様の変化の際にモデルの作り直しが発生し，回帰的な検証を効果的に実施できない．第 2 は検証結果の解釈である．検証用モデルに対する検証結果が業務要件とシステム仕様にどう該当するのか明確ではない．

業務要件の形式検証の将来像

図 -2 に，業務要件検証への形式手法の効果的な適用のイメージを示す．「一品ものモデル」の問題の回避策として，形式検証器非依存な形式で記述し，個別の形式検証器向けの検証用モデルの生成のベースとなる「検証マザーモデル」を導入する．検証用モデルの生成と検証結果の解釈を検証エンジンにおいて自動化し，スキル習熟コストを大きく低減する．

業務要件は，問題領域(ドメイン)と情報システム間に起こる，外部から観測可能な相互作用に関する制約と考える [1), 2)]．ドメインとシステム双方の記述があって初めて業務要件が表現できる．両者の相互作用を表現するため，ドメインとシステムの 2 つのサブモデルを検証マザーモデルの主要構成要素とする．ドメインモデルには人間，組織，データ，他システムなどの，システムとの間に相互作用を持つ要素を記述する．

ドメインモデルとシステムモデルを分けることで，回帰的な検証時のモデル修正を局所化できる．たとえば法制度や業務ルールの変化をドメインモデルに反映し，現状システムでの対応状況を確認できる．また，システム保守時の修正をシステムモデルに反映することで，修正内容が既存の業務要件に与える影響を検証できる．

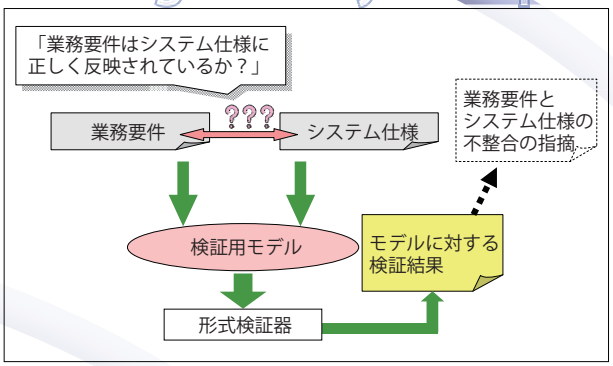

図 -1　従来の形式手法適用イメージ

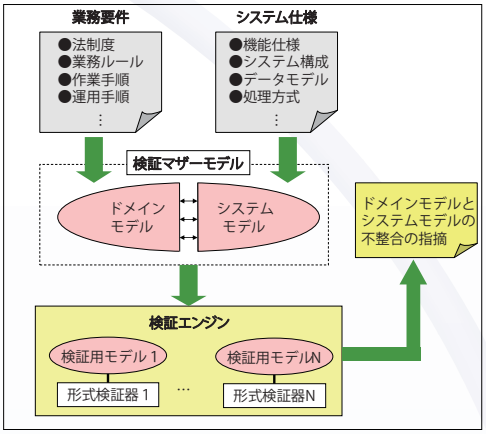

図 -2　業務要件検証への形式手法適用イメージ

図 -2 のスタイルでの業務要件の形式検証の実現性を示す研究として文献 3）がある．ジョブ管理分野における処理フローに対する検証マザーモデルを状態遷移機械ベースで記述する．処理フロー実行のいかなる場面でも，ドメインの状態が適正であること（処理フローが不正な相互作用をドメインに対して行わないこと）を検証できるツールの試作である．形式検証器としては Spin を用いている．

業務要件の形式検証には，問題領域のモデリング技術，モデル生成技術，形式検証技術や，高い使用性を持った開発環境，開発プロセス，モデル管理技術など，ソフトウェア工学の多くの側面の融合が必要である．本会がそのような融合を促進する活発な産学連携の場であり続けるよう期待する．

参考文献

1）Jackson, M. : The World and the Machine, Proc. ICSE'95, pp.283-292 (1995).
2）二木厚吉：フォーマルメソッドの新展開　検証進化可能電子社会の中核技術，情報処理，Vol. 49, No.5, pp. 521-529 (May 2008).
3）森岡　剛：処理フロー正当性の早期検証ツールの提案，電気学会 情報システム研究会，IS-09-73 (2009).

（平成 21 年 10 月 30 日受付）

森岡　剛●
2005 年 Univ. of Toronto にて Ph.D.（Computer Science）取得．同年（株）日立製作所入社．現在システム開発研究所研究員．システムアーキテクチャ，システム生産技術．

三部良太(正会員)●
1992 年東京工業大学大学院総合理工学研究科情報工学専攻修士課程修了．同年より（株）日立製作所システム開発研究所．一貫してソフトウェア生産性の研究に従事．